




NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

1

CISCO SYSTEMS






Network Troubleshooting Tools and Techniques

Session NCM-301

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

3

Agenda



- **Overview**
- **Troubleshooting Techniques**
- **Tools of the Trade**
- **Case Studies**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

4

Troubleshooting Overview

Cisco.com

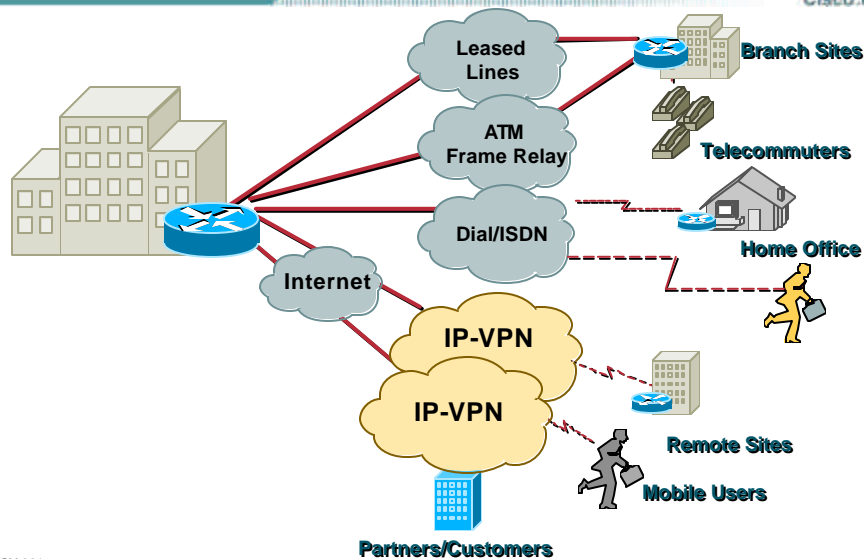
- Troubleshooting in today's complex networks
- Troubleshooting is a two-part process

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

5

Today's Complex Networks

Cisco.com



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

6

Troubleshooting Is a Two-Part Process

Cisco.com

- **Know and understand your network**
- **Be prepared when problems arise**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

7

Baseline Your Network

Cisco.com

- **Gather device software versions**
 - Show version
 - Show module
- **Gather device configurations**
 - Show run
 - Show config all
- **Gather device statistics**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

8

Gather Device Statistics

Cisco.com

- **Collect stats for utilization as well as errors**
- **Trend this data over time**



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

9

Baselining (Cont.)

Cisco.com

- **Make a logical map of your network**
- **Know the protocols that are running on your network**

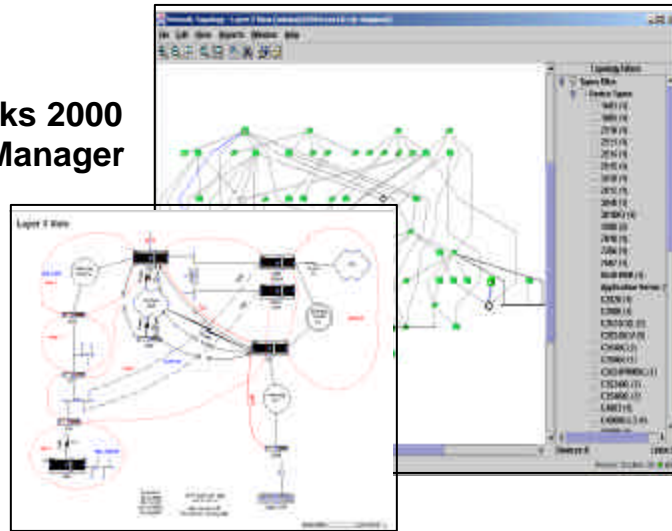
NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

10

Make a Logical Map of Your Network

Cisco.com

- CiscoWorks 2000 Campus Manager
- Visio



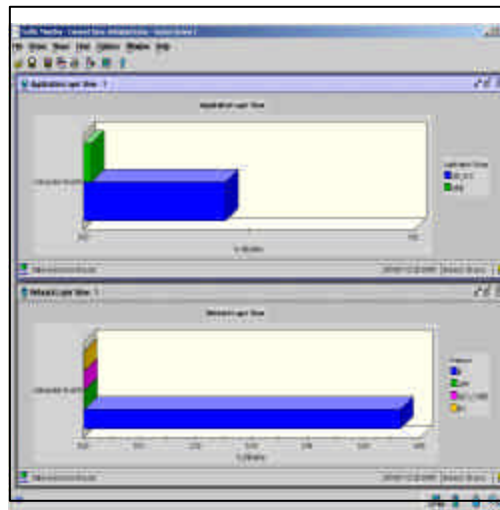
NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

11

Know the Protocols That Are Running on Your Network

Cisco.com

- RMON
- Packet sniffers



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

12

So You Have a Problem

Cisco.com

- Have your network baseline on hand
- **Don't panic**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

13

Gather All Information

Cisco.com

- Listen to your users
 - “It's taking **forever** to **transfer** this file”
 - “Is the **server down**?”
- Ask the right questions
 - “Do other files transfer quickly?”
 - “Can you connect to other servers?”

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

14

Classify the Problem

Cisco.com

- **Connectivity**
- **Performance**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

15

Causes of Connectivity Problems

Cisco.com

- **Faulty hardware or media**
- **Bugs**
- **Backhoes cutting fiber**
- **Power outages**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

16

Causes of Performance Problems

Cisco.com

- Network congestion
- Less desirable route to destination
- Underpowered network devices
- Network faults such as a spanning tree loops
- Network noise or errors

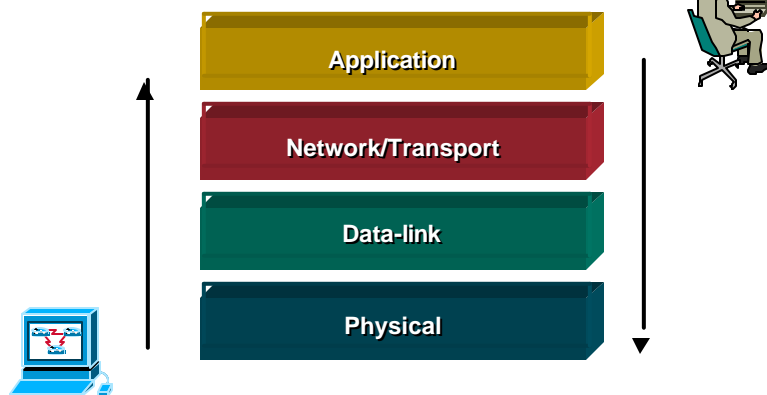
NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

17

Develop a Plan of Attack

Cisco.com

Bottom-up or Top-down?

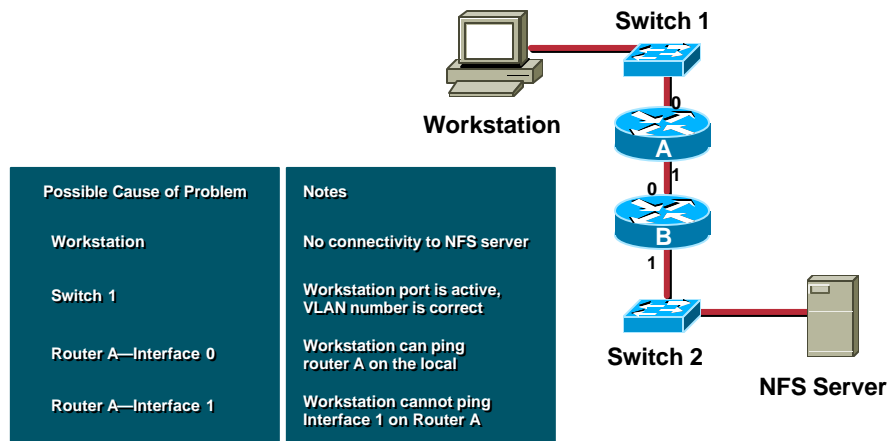


NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

18

Document Your Actions

Cisco.com



Don't Introduce New Problems!

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

19

Work As a Team

Cisco.com



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

20

Agenda

Cisco.com

- Overview
- Troubleshooting Techniques
- **Tools of the Trade**
- Case Studies

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

21

Tools of the Trade

Cisco.com

- General tools
- Cisco-specific tools

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

22

Tools of the Trade—General

Cisco.com

- **Ping**
- **Traceroute**
- **Pchar**
- **Netcat**
- **Nslookup**
- **Packet Sniffers**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

23

Ping

Cisco.com

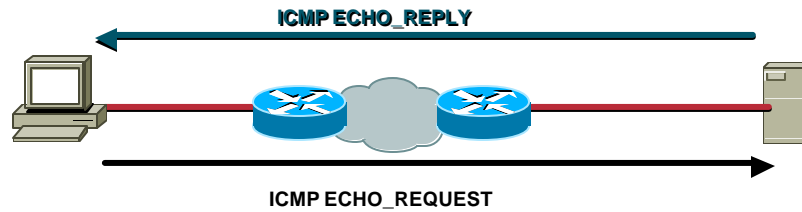
- **Everywhere you go, there's ping**
- **Check end-to-end network connectivity**
- **Baseline network layer performance**
- **Find data-dependent problems**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

24

Ping Example—Success

Cisco.com



```
PING rtp-cse-181.cisco.com (64.102.55.45): 56 data bytes
64 bytes from 64.102.55.45: icmp_seq=0 ttl=250 time=0.667 ms
^C
--- rtp-cse-181.cisco.com ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.667/0.667/0.667/0.000 ms
```

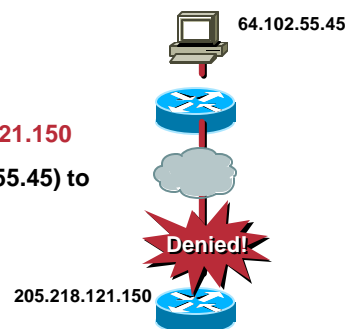
NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

25

Ping Example—Packets Blocked

Cisco.com

```
PING 205.218.121.150: 56 data bytes
ICMP 13 Unreachable from gateway 205.218.121.150
for icmp from rtp-cse-181.cisco.com (64.102.55.45) to
205.218.121.150
```



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

26

ICMP Types and Codes

Cisco.com

ICMP Type	ICMP Code
0—Echo Reply	0—None
3—Unreachable	0—Network Unreachable
	1—Host Unreachable
	2—Protocol Unreachable
	3—Port Unreachable
	4—Fragment Needed and DF Bit Set
	5—Source Route Failed
	6—Network Unknown
	7—Host Unknown
	8—Source Host Isolated
	9—Communication With Destination Network Is Administratively Prohibited
	10—Communication With Destination Host Is Administratively Prohibited
	11—Bad Type of Service for Destination Network
	12—Bad Type of Service for Destination Host
	13—Administratively Blocked by Filter

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

27

Ping Options

Cisco.com

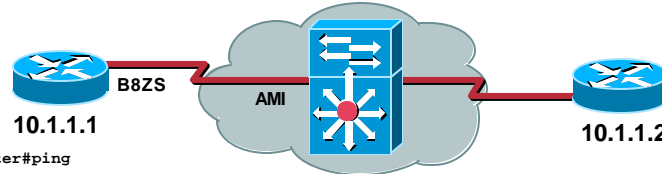
Ping Option	OS Availability	Notes
Repeat Count	UNIX, Windows, IOS	Generate Extended Amounts of Network Traffic Stress-Test Response Time or Network Connectivity
Flood	Unix	Generate Packets As Quickly As Possible Get an Idea of How Many Packets Are Being Dropped Due to Its Danger, Usually Only Available to Super-User
Data Pattern	UNIX, IOS	Change the Data Pattern to Test for Data-dependent Problems Such As T1 Timing or Line Code Problems
Packet Size	UNIX, Windows, IOS	Increase Packet Size to Help Identify Data-dependent Problems Useful for Networklayer Packet Generation
Source Interface	Unix, IOS	Verify Proper Routing Test That Services Like NAT Are Working Correctly

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

28

Ping Example—T1 Line Code Violation

Cisco.com



```
Router#ping
Protocol [ip]:
Target IP address: 10.1.1.2
Repeat count [5]: 100
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0x0000
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet has data pattern 0x0000
!!!!!!!!!!!!!!!!!!!!.U.U..U!!!!!!!!!!!!!!!!!!!!.U.U!!!!!!!!!!!!.
U.U.U!!!!!!!!!!!!
```

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

29

Ping Drawbacks

Cisco.com

- Increases network load
- Uses artificially high TTL value
- Often routers lower the priority for ping to prevent DoS attacks
- Only does network-layer checks
- Does not pinpoint network problems

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

30

Traceroute

Cisco.com

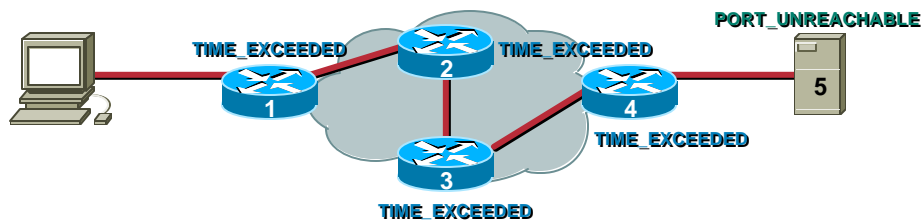
- Uses IP TTL field to discover gateways
 - UDP probes sent to high ports
 - Elicits ICMP TIME_EXCEEDED from gateways
 - Elicits ICMP PORT_UNREACHABLE from destination
- Narrow down connectivity issues
- Baseline network layer performance on a hop-by-hop basis

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

31

Traceroute Example

Cisco.com



traceroute to nms-server2.cisco.com (172.18.124.33), 30 hop max, 40 byte packets

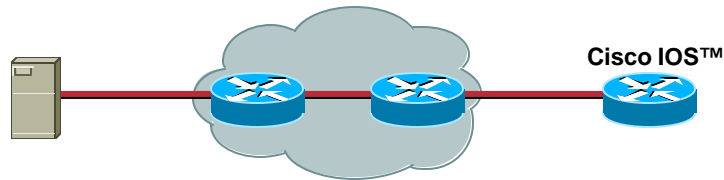
- 1 rtp5-gw1.cisco.com (64.102.55.2) 3.06 ms 0.533 ms 0.584 ms
- 2 rtp5-bb-gw1.cisco.com (10.81.254.73) 1.533 ms 0.393 ms 0.345 ms
- 3 rtp7-lab-gw1.cisco.com (10.81.254.66) 1.482 ms 0.55 ms 0.518 ms
- 4 172.18.127.134 (172.18.127.134) 5.224 ms 4.94 ms 4.427 ms
- 5 nms-server2.cisco.com (172.18.124.33) 4.865 ms 5.565 ms 5.049 ms

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

32

Traceroute Example— Destination: Cisco

Cisco.com



traceroute to 10.29.4.1 (10.29.4.1), 30 hops max, 40 byte packets

```
1  nms-2511.rtp.cisco.com (10.29.100.2) 2.278 ms 2.088 ms 2.488 ms
2  nms-2610a.rtp.cisco.com (10.29.100.5) 3.363 ms 3.071 ms 3.153 ms
3  10.29.3.2 (10.29.3.2) 17.060 ms * 15.721 ms
```

Throttle

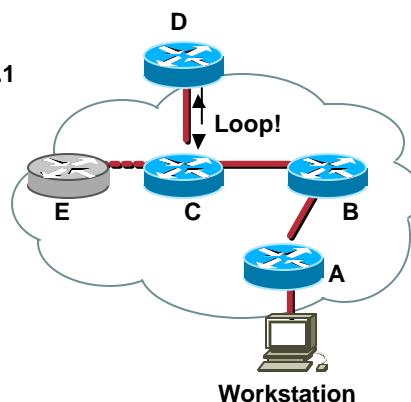
NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

33

Traceroute Example—Routing Loop

Cisco.com

```
rtrE workstation# traceroute 10.29.254.1
1 10.29.100.2 2 ms 2 ms 2 ms
2 10.29.2.1 5 ms 2 ms 3 ms
3 10.29.1.1 4 ms 1 ms 1 ms
rtrC 4 10.1.3.30 46 ms 51 ms 49 ms
rtrD 5 10.29.1.1 52 ms 46 ms 30 ms
rtrC 6 10.1.3.30 12 ms 26 ms 7 ms
```



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

34

Traceroute Options

Cisco.com

Traceroute Option	OS Availability	Notes
Probe Port Number	UNIX	Useful to Change If the Destination Host Is Listening on the Default Probe Port (Usually 33434)
Maximum Number of Hops	UNIX, Windows	Increase This If the Destination Host Is Further Away Than the Default of 30 Hops If This Has to Go Above 64, There Is Usually a Routing Problem
Source Interface/ Address	UNIX	Verify That Routing Works From the Given Address Verify Services Like NAT Are Working Correctly

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

35

Traceroute Availability

Cisco.com

- Available for most platforms
- Source code downloadable from <http://ee.lbl.gov>

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

36

Traceroute Drawbacks

Cisco.com

- **ICMP messages may be filtered**
- **Different IP stacks respond differently to traceroute**
- **Latency figures may not be accurate with regard to applications**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

37

Pchar

Cisco.com

- **Based on pathchar (path characterization tool by Van Jacobson)**
- **Measures network performance on a per-hop and a total path basis**
- **Supports IPv4 and IPv6**
- **Useful in isolating performance problems**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

38

Pchar Example—Hop Statistics

Cisco.com



0: 10.29.100.33 (nms-server2.rtp.cisco.com)

Partial loss: 1 / 1472 (0%)

Partial char: rtt = 1.872604 ms, (b = 0.000876 ms/B), r2 = 0.998560
stddev rtt = 0.004053, stddev b = 0.000005

Partial queuing: avg = 0.001308 ms (1492 bytes)

Hop char: rtt = 1.872604 ms, bw = 9130.730297 Kbps

Hop queuing: avg = 0.001308 ms (1492 bytes)

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

39

Pchar Example—Path Statistics

Cisco.com



Path length: 4 hops

Path char: rtt = 4.692853 ms r2 = 0.999996

Path bottleneck: 126.277240 Kbps

Path pipe: 74 bytes

Path queuing: average = 0.003377 ms (1582 bytes)

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

40

Pchar Options

Cisco.com

Pchar Flag	Notes
-c	Ignore Routing Changes Useful in Situations Where Load-balancing Is Used
-p	Specify the Protocol That pchar Uses This Can Be ipv4udp (Default), ipv4raw, ipv4icmp, ipv4tcp, ipv6icmp or ipv6udp
-S	Do SNMP Queries at Each Hop to Determine Each Router's Idea of What It Thinks the Next-hop Interface Characteristics Are This Option Requires the Net-snmp Libraries From ftp://ucd-snmplib.ucdavis.edu

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

41

Pchar Drawbacks

Cisco.com

- ICMP messages may be filtered
- Different IP stacks respond differently to pchar
- Latency figures may not be accurate with regard to applications

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

42

Pchar Availability

Cisco.com

- Pchar source code can be downloaded from:
<http://www.employees.org/~bmah/Software/pchar>
- Tested on FreeBSD, NetBSD, OpenBSD, Linux, Solaris, IRIX, and OSF/1 (Tru64)

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

43

Netcat

Cisco.com

- Similar in operation to telnet
- Tests application connectivity
- Can test TCP and UDP services

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

44

Netcat Example— Verify HTTP Connectivity

Cisco.com



```
% nc -v -w 3 nms-server2.cisco.com 80
nms-server2.cisco.com [172.18.124.33] 80 (http) open
GET / HTTP/1.0
HTTP/1.1 200 OK
[HTML data]
```

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

45

Netcat Example— Verify Syslog Connectivity

Cisco.com



```
% echo '<38>Hello World' | nc -w 1 -u nms-server2 514
% tail -1 /var/log/messages
Apr 17 00:54:45 nms-server2 Hello World
```

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

46

Netcat Options

Cisco.com

- Use “nc -v -w 3” for verifying TCP services

Pchar Flag	Notes
-w	Change the Network Inactivity Timeout Changing This to at Least 3 Is Useful When Checking Web or Gopher Services
-u	Tell Netcat to Use UDP Instead of TCP Netcat Will Simulate a UDP “Connection”
-l	Cause Netcat to Listen at a Given Port (As Specified With the -p Flag) This Option Is Useful for Creating Mock Services to Test Throughput or Connectivity Use With the -u Flag to Create a UDP Server
-p, -s	When Netcat Is Run With the -l Flag, Use the Specified Port and IP Address Respectively

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

47

Netcat Drawbacks

Cisco.com

- Does not measure network performance
- Does not attempt to isolate where the connectivity problem lies in the network

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

48

Netcat Availability

Cisco.com

- Source code can be downloaded from:
<ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/netcat/>
- Windows binary available from:
<http://www.atstake.com/research/tools/index.html>

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

49

NSLookup

Cisco.com

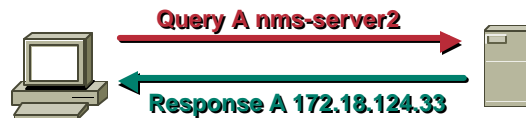
- Used to query Domain Name Service for IP addresses and hostnames
- Client-side DNS failures gives a false positive for a connectivity problem
- Server-side DNS failures can cause sluggish service connection times

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

50

Nslookup Example— Verify Name and Address Match

Cisco.com



```
% nslookup nms-server2
Server: redclay2.cisco.com
Address: 172.18.125.3
```

```
% nslookup 172.18.124.33
Server: redclay2.cisco.com
Address: 172.18.125.3
```

```
Name: nms-server2.cisco.com
Address: 172.18.124.33
```

```
Name: nms-server2.cisco.com
Address: 172.18.124.33
```

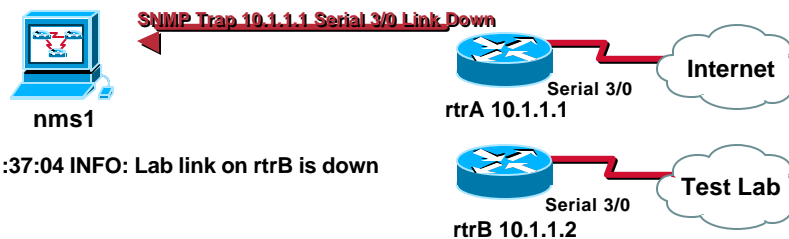
Queries Match

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

51

NSLookup Example— Address and Name Do Not Match

Cisco.com



Apr 25 11:37:04 INFO: Lab link on rtrB is down

```
nms1> nslookup rtrA
Server: dns-server
Address: 10.1.1.4
```

```
Name: rtrA
Address: 10.1.1.1
```

```
nms1> nslookup 10.1.1.1
Server: dns-server
Address: 10.1.1.4
```

```
Name: rtrB
Address: 10.1.1.1
```

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

52

NSLookup Options

Cisco.com

- Use the **-qt=<query type>** command line flag to test different kinds of records

Query Type	Type of Record Returned
A	The Host's IP Address
CNAME	The Canonical Name for an Alias
MX	The Mail Exchanger for the Given Domain
PTR	The Host Name If the Query Is an IP Address; Otherwise the Pointer to Other Information
SOA	Start of Authority—The Actual Domain Name Server That Hosts the Given Domain

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

53

Packet Sniffers

Cisco.com

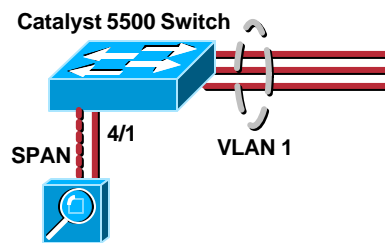
- Analyze what's really happening on the wire
- Good for measuring performance and connectivity
- Helpful for establishing network baselines

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

54

Packet Sniffers— Setup in a Switched Network

Cisco.com



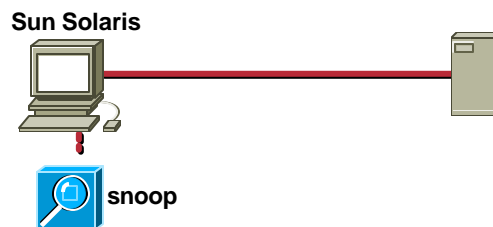
set span 1 4/1

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

55

Packet Sniffers—snoop

Cisco.com



snoop jclarke-sun and tcp port 23

Using device /dev/hme (promiscuous mode)

rtp-cse-181.cisco.com -> rtp-dogwood.cisco.com TELNET C port=55083

rtp-dogwood.cisco.com -> rtp-cse-181.cisco.com TELNET R port=55083

Using device /dev/hm

rtp-cse-181.cisco.com -> rtp-dogwood.cisco.com TELNET C port=55083

rtp-dogwood.cisco.com -> rtp-cse-181.cisco.com TELNET R port=55083 rtp-cse-181.cisco.co

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

56

Packet Sniffers—tcpdump

Cisco.com

tcpdump host jclarke-sun and tcp port 23
tcpdump: listening on fxp0

12:21:37.298373 nms-server2.cisco.com.telnet > rtp-cse-181.cisco.com.51027: P
344418520:344418548(28) ack 2892313522 win 17520 (DF) [tos 0x10]

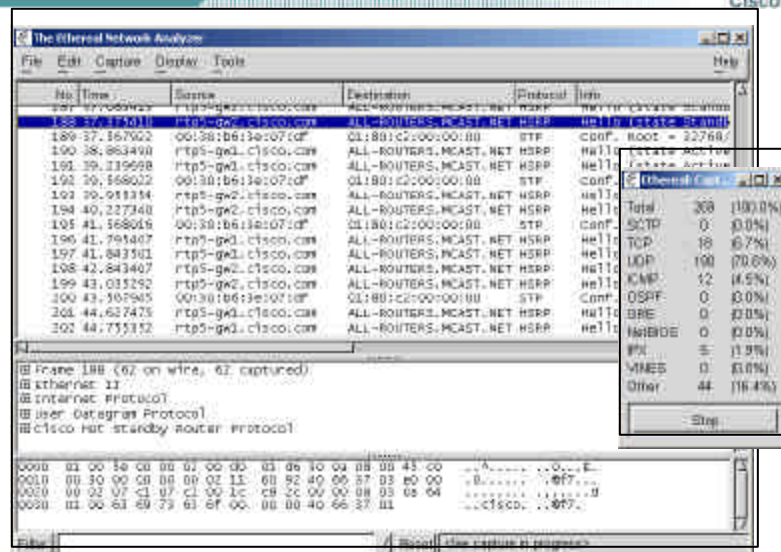
- Source code available from <http://ee.lbl.gov>

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

57

Packet Sniffers—Ethereal

Cisco.com



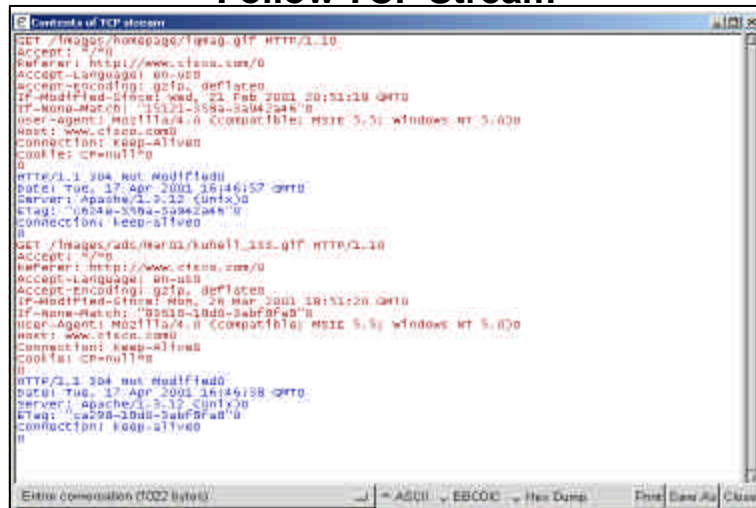
NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

58

Packet Sniffers—Ethereal

Cisco.com

Follow TCP Stream



```
Contents of TCP stream
GET /images/homepage/logo.gif HTTP/1.1.0
Accept: */*
Referer: http://www.cisco.com/0
Accept-Language: en-us
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 22 Feb 2001 20:53:19 GMT
If-None-Match: "15121-559a-5a942a4"
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; windows NT 5.0)
Host: www.cisco.com
Connection: keep-alive
Cookie: CP=01190
HTTP/1.1 204 Not Modified
Date: Tue, 17 Apr 2001 16:46:52 GMT
Server: Apache/1.3.12 (Unix)
Etag: "15121-559a-5a942a4"
Connection: keep-alive

GET /images/ads/home/133.gif HTTP/1.1.0
Accept: */*
Referer: http://www.cisco.com/0
Accept-Language: en-us
Accept-Encoding: gzip, deflate
If-Modified-Since: Mon, 26 Mar 2001 18:11:20 GMT
If-None-Match: "20310-10d0-2abf0ab"
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; windows NT 5.0)
Host: www.cisco.com
Connection: keep-alive
Cookie: CP=01190
HTTP/1.1 204 Not Modified
Date: Tue, 17 Apr 2001 16:46:58 GMT
Server: Apache/1.3.12 (Unix)
Etag: "20310-10d0-2abf0ab"
Connection: keep-alive
```

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

59

Packet Sniffers—Ethereal

Cisco.com

- Reads traces from most commercial packet sniffers
- Reads snoop and tcpdump capture files
 - snoop -s 1518 -o outfile
 - tcpdump -s 1518 -w outfile
- Freely available from <http://www.ethereal.com>

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

60

Tools of the Trade—Cisco

Cisco.com

- **Show commands**
- **Debugs**
- **Cisco Service Assurance Agent (SAA)**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

61

Show Commands

Cisco.com

- **show cam dynamic**
- **show cdp neighbor**
- **show ip route**
- **show ip cef**
- **show process cpu**
- **show system**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

62

show cam dynamic

Cisco.com

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN	Dest MAC/Route Des	[CoS]	Destination Ports or VCs / [Protocol Type]
----	-----	----	-----
18	00-10-0d-38-10-00		5/3 [ALL]
6	00-30-94-1c-46-ff		5/3 [ALL]
100	00-90-27-86-76-e2		5/1 [ALL]
18	00-00-0c-07-ac-12		5/3 [ALL]
100	00-04-de-a9-18-00		5/3 [ALL]
6	00-04-4e-f2-c8-00		5/3 [ALL]
19	00-10-0d-a1-18-80		5/3 [ALL]

- Catalyst OS command
- Shows MAC to port mapping

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

63

Cisco Discovery Protocol

Cisco.com

- Uses layer 2 multicast for advertisements
- Uses special multicast MAC address so that Cisco devices will not forward CDP packets

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

64

Cisco Discovery Protocol (Cont.)

Cisco.com

- **Runs on virtually all Cisco devices**
- **Enabled by default on all broadcast interfaces**
- **Displays information about directly connected neighbors**
- **Useful for debugging connectivity issues as well as building topology maps**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

65

CDP Rules of Thumb

Cisco.com

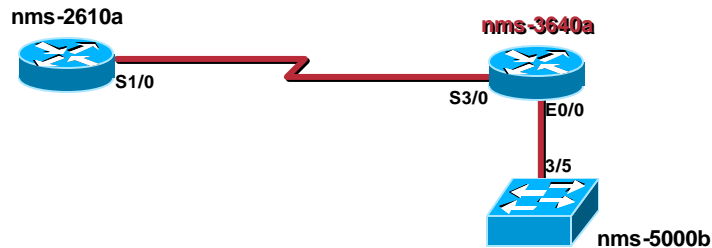
- **Configure CDP only on links between Cisco devices**
- **Do not configure CDP on links you do not manage**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

66

show cdp neighbor

Cisco.com



nms-3640a#show cdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
009042675(nms-5000b)	Eth 0/0	152	T B S	WS-C5000	3/5
nms-2610a.rtp.cis	Se 3/0	169	R	2610	Se 1/0

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

67

show cdp neighbor detail

Cisco.com



ID: 009042675(nms-5000b)
Entry address(es):
IP address: 10.29.4.10
Platform: WS-C5000, Capabilities: TransBridge Source-Route-Bridge Switch
Interface: Ethernet0/0, Port ID (outgoing port): 3/5
Holdtime : 174 sec

Version :
WS-C5000 Software, Version McpSW: 5.4(4) NmpSW: 5.4(4)
Copyright (c) 1995-2000 by Cisco Systems

advertisement version: 2
VTP Management Domain: 'nms-remote'
Native VLAN: 4
Duplex: full

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

68

show ip route

Cisco.com

Gateway of last resort is 10.29.3.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 27 subnets, 4 masks

```
O 10.29.22.0/24 [110/110] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.5.16/30 [110/160] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.19.0/24 [110/137] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.18.0/24 [110/137] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.5.20/30 [110/135] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.5.24/30 [110/160] via 10.29.4.2, 12:09:27, Ethernet0/0
O E2 10.29.7.0/24 [110/20] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.5.2/32 [110/110] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.6.0/24 [110/136] via 10.29.4.2, 12:09:27, Ethernet0/0
O IA 10.29.5.3/32 [110/135] via 10.29.4.2, 12:09:27, Ethernet0/0
O E2 10.29.5.0/28 [110/40] via 10.29.4.2, 12:09:27, Ethernet0/0
```

- Verify all routers have a route to the destination
- Verify that the route taken is optimal

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

69

show ip cef

Cisco.com

Prefix	Next Hop	Interface
0.0.0.0/0	10.29.5.33	Serial15/0/0.2
	10.29.5.1	Serial15/0/0.1
0.0.0.0/32	receive	
10.29.1.0/24	10.29.5.33	Serial15/0/0.2
	10.29.5.1	Serial15/0/0.1
10.29.2.0/24	10.29.5.33	Serial15/0/0.2
	10.29.5.1	Serial15/0/0.1
10.29.3.0/24	10.29.5.33	Serial15/0/0.2
	10.29.5.1	Serial15/0/0.1
10.29.4.0/24	10.29.5.33	Serial15/0/0.2
	10.29.5.1	Serial15/0/0.1
10.29.5.0/28	attached	Serial15/0/0.1
10.29.5.0/32	receive	

- Verify next hops and interfaces are correct for given route prefixes
- Corrupted CEF tables can cause strange routing behaviors

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

70

show process cpu

Cisco.com

CPU utilization for five seconds: 29%/6%; one minute: 8%; five minutes: 5%

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
1	880	1823462	0	0.00%	0.00%	0.00%	0	Load Meter
2	572128	2351401	243	0.00%	0.00%	0.00%	0	OSPF Hello
3	0	106	0	0.00%	0.00%	0.00%	0	RTR Scheduler
4	6118648	1117174	5476	0.00%	0.08%	0.10%	0	Check heaps
5	0	1	0	0.00%	0.00%	0.00%	0	Chunk Manager
6	0	2	0	0.00%	0.00%	0.00%	0	Pool Manager
7	0	2	0	0.00%	0.00%	0.00%	0	Timers
8	0	36	0	0.00%	0.00%	0.00%	0	Serial Backgroun
9	0	1	0	0.00%	0.00%	0.00%	0	OIR Handler
10	1832	112	16357	30.01%	10.03%	7.44%	18	Virtual Exec

- Check to make sure overall system load is under control
- Use the process list to determine which process might be misbehaving

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

71

show system

Cisco.com

```
PS1-Status PS2-Status
-----
ok         none

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
-----
ok         off         ok         7,07:46:16    20 min

PS1-Type          PS2-Type
-----
WS-CAC-1000W      none

Modem  Baud  Traffic Peak Peak-Time
-----
disable 9600 5%      7% Thu May 3 2001, 10:06:00

PS1 Capacity: 852.60 Watts (20.30 Amps @42V)

System Name          System Location          System Contact          CC
-----
"NMS Pod"
```

- Catalyst OS command
- Shows environmental stats as well as peak and current traffic load

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

72

Debugs

Cisco.com

- Debug ip packet detail
- Debug ip routing

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

73

debug ip packet detail

Cisco.com

```
1w2d: IP: s=172.18.124.189 (Serial5/0/0.2), d=10.29.8.2, len 425, rcvd 4
1w2d:   UDP src=47427, dst=161
1w2d: IP: s=172.18.124.189 (Serial5/0/0.2), d=10.29.8.2, len 416, rcvd 4
1w2d:   UDP src=47427, dst=161
1w2d: IP: s=172.18.124.189 (Serial5/0/0.2), d=10.29.8.2, len 415, rcvd 4
1w2d:   UDP src=47427, dst=161
1w2d: IP: s=172.18.124.189 (Serial5/0/0.2), d=10.29.8.2, len 417, rcvd 4
1w2d:   UDP src=47427, dst=161
1w2d: IP: s=172.18.124.189 (Serial5/0/0.2), d=10.29.8.2, len 424, rcvd 4
1w2d:   UDP src=47427, dst=161
1w2d: IP: s=172.18.124.189 (Serial5/0/0.2), d=10.29.8.2, len 424, rcvd 4
1w2d:   UDP src=47427, dst=161
```

- Useful for verifying packet throughput when a sniffer is not available
- **Can crash a busy router if not used carefully!**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

74

debug ip packet detail <acl>

Cisco.com

```
router# debug ip packet detail ?
<1-199>      Access list
<1300-2699>  Access list (extended range)
<cr>
```

Use an Access-List to Limit the Output!

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

75

debug ip routing

Cisco.com

```
15w0d: RT: add 10.29.6.0/24 via 10.29.3.1, ospf metric [110/792]
15w0d: RT: add 10.29.18.0/24 via 10.29.3.1, ospf metric [110/792]
15w0d: RT: add 10.29.19.0/24 via 10.29.3.1, ospf metric [110/793]
15w0d: RT: add 10.29.41.0/24 via 10.29.3.1, ospf metric [110/792]
15w0d: RT: add 10.29.42.0/24 via 10.29.3.1, ospf metric [110/792]
15w0d: RT: add 10.29.100.0/24 via 10.29.3.1, ospf metric [110/791]
```

- See when routes are added and deleted from the routing table
- Encompasses all routing protocols

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

76

debug ip routing <acl>

Cisco.com

```
router# debug ip routing ?  
  <1-199>           Access list  
  <1300-2699>       Access list (extended range)  
  <cr>
```

- Use access-lists to limit the output and to focus on specific routes

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

77

Cisco Service Assurance Agent (SAA)

Cisco.com

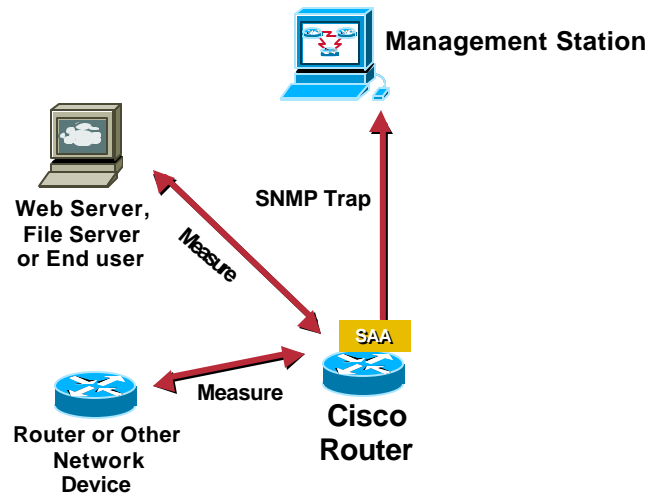
- LAN/WAN troubleshooting
 - Measures hop-by-hop response time and availability
 - Evaluates thresholds and generates alarms
 - QoS aware
- Utilizes SA agent embedded in IOS
 - No extra management hardware required
 - Leverage your existing Cisco routers

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

78

SAA Operations

Cisco.com



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

79

SAA Example Use

Cisco.com

- QoS
 - ToS Settings
 - ICMP, UDP Echo port
 - Jitter
 - TCP Connect
 - HTTP
- Non QoS
 - Network Services
 - DNS
 - DHCP
- Two hour histories
- Real time
- Hop-by-hop path analysis
- Trap notification

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

80

SAA Availability

Cisco.com



SA Agent

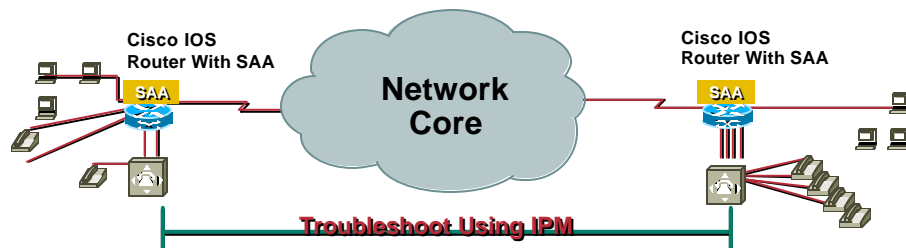
- IOS 11.2 (18)
- IOS 11.3 (6)
 - IP Plus
 - Desktop Plus
 - IBM
 - Enterprise
- IOS 12.0(5)
- IOS 12.0(5)T
- IOS 12.1(1)

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

81

How SAA Works

Cisco.com



SAA Benefits

- No extra management hardware required
- Proactive as well as reactive
- Baseline network performance
- Service-aware transactions closely match real-life service performance

Metrics Measured

- Response time
- Availability
- Jitter
- Packet loss

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

82

Internetwork Performance Monitor

Cisco.com



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

83

Agenda

Cisco.com

- Overview
- Troubleshooting Techniques
- Tools of the Trade
- **Case Studies**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

84

Case Study 1: Resource Manager Essentials Config Retrieval

Cisco.com

- Problem: RME **cannot collect** configurations from my devices

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

85

How It Should Work

Cisco.com



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

86

Cisco.com

The diagram illustrates a network topology where a central management station, labeled 'CiscoWorks 2000', is connected to two separate network segments. On the left, a cluster of four blue routers is associated with the IP range '10.30.x.x'. On the right, another cluster of four blue routers is associated with the IP range '10.29.x.x'. Red lines represent the network connections between the central laptop and the router clusters.

87

Cisco.com

88

Ask the Right Questions

Cisco.com

- **Does this work for any devices?**
Yes, it works for devices on the 10.30.x.x subnet
- **Can you do a manual TFTP from the failing devices to the server?**
Yes, manually doing a copy running tftp works fine

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

89

Develop a Plan of Attack

Cisco.com

- **TFTP operations work to the 10.30.x.x subnet**
Assumption: CiscoWorks 2000 services are working correctly, and the TFTP daemon is functioning
- **Manual TFTP operations work for the devices failing in CiscoWorks 2000**
Assumption: Network and TFTP application layer connectivity exists between the failing devices
- **Next step: Get a sniffer and analyze what is happening on the wire**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

90

Document Your Actions

Cisco.com



CiscoWorks 2000

Action	Notes
Updated CW2000 Configuration Archive for 10.30.1.1	Operation Succeeded; Running Config Was Archived Via TFTP
Tried Manual TFTP From 10.29.X.X Subnet	Manual TFTP Operation Succeeds
Place a Sniffer on the 10.29.X.X Subnet	We Need to Determine What Is Happening on the Wire Between the CW2000 Machine and the Failing Device

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

91

Sniffing the Wire

Cisco.com

Internet Protocol

Source: **10.29.100.37** (rtp-redwood)

Destination: 10.29.4.2 (nms-4000b)

Simple Network Management Protocol

Version: 1

Community: private

PDU type: SET

Request Id: 0xf11

Error Status: NO ERROR

Error Index: 0

Object identifier 1: 1.3.6.1.4.1.9.2.1.55. **10.30.100.37** (OLD-CISCO-SYS-MIB::writeNet.**10.30.100.37**)

Value: OCTET STRING: 20010320145845-10.29.4.2.cfg

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

92

Sniffing the Wire (Cont.)

Cisco.com

Internet Protocol

Version: 4

Source: 10.29.4.2 (nms-4000b)

Destination: 10.30.100.37 (rtp-redwood)

Trivial File Transfer Protocol

Opcode: Write Request (2)

DESTINATION File: 20010320145845-10.29.4.2.cfg

Type: octet

Internet Protocol

Version: 4

Source: 10.29.100.37 (rtp-redwood)

Destination: 10.29.4.2 (nms-4000b)

Internet Control Message Protocol

Type: 3 (Destination unreachable)

Code: 9 (Network administratively prohibited)

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

93

Problem Solved!

Cisco.com

- **Solution: The fact that the CiscoWorks 2000 machine is multi-homed is causing a problem with Resource Manager Essentials; calling the TAC reveals this is bug CSCdp30606 which is fixed in RME 3.2**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

94

Case Study 2: Troubleshooting Mobile IP

Cisco.com

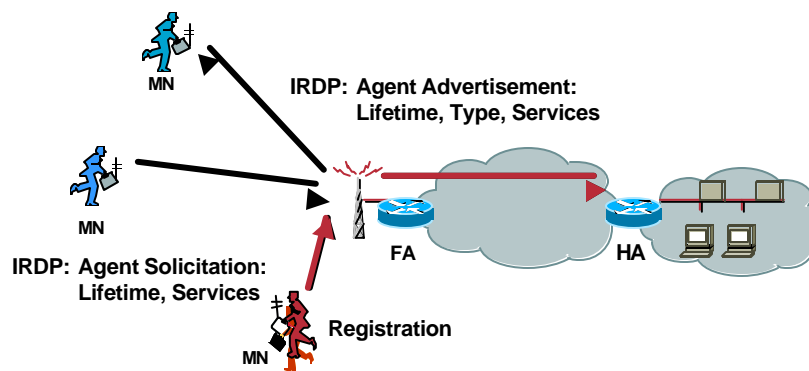
- Problem: Mobile nodes are taking a **long time** to get registered with the home agent

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

95

How It Should Work

Cisco.com

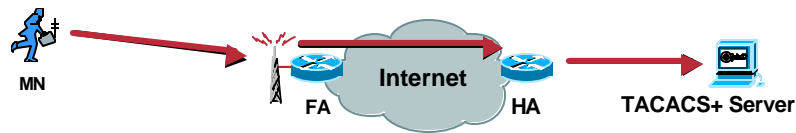


NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

96

Know Your Topology

Cisco.com



- Mobile node registration comes in to the home agent via the foreign agent
- The home agent checks the remote TACACS+ authentication database to verify that the mobile node is allowed to register

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

97

What Are the Symptoms?

Cisco.com

- Mobile nodes retry multiple times before successfully registering with home agent
- Sometimes the mobile node needs to be rebooted before it will successfully register

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

98

Ask the Right Questions

Cisco.com

- Does this happen all the time?
No, only when a large number of mobile nodes try to register at the same time
- Do you see any errors on the home agent when these failures are occurring?
Yes, we see “insufficient resources” errors incrementing when this problem occurs
- Does the home agent CPU spike when this problem is occurring?
No, CPU stays relatively low on the HA

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

99

Develop a Plan of Attack

Cisco.com

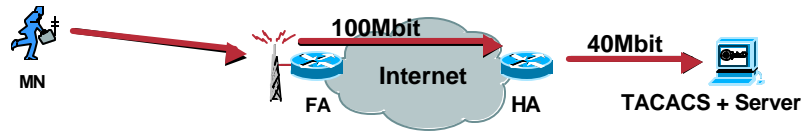
- Mobile node registrations timeout when a large number of registrations take place at once
Assumption: Somewhere we are hitting a bottleneck
- “Insufficient resources” errors are incrementing when failures occur
Assumption: This supports our bottleneck assumption
- CPU remains stable on the home agent
Assumption: The HA itself is not the bottleneck
- Next step: Analyze the paths between the HA and the FA and between the HA and the TACACS server

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

100

Document Your Actions

Cisco.com



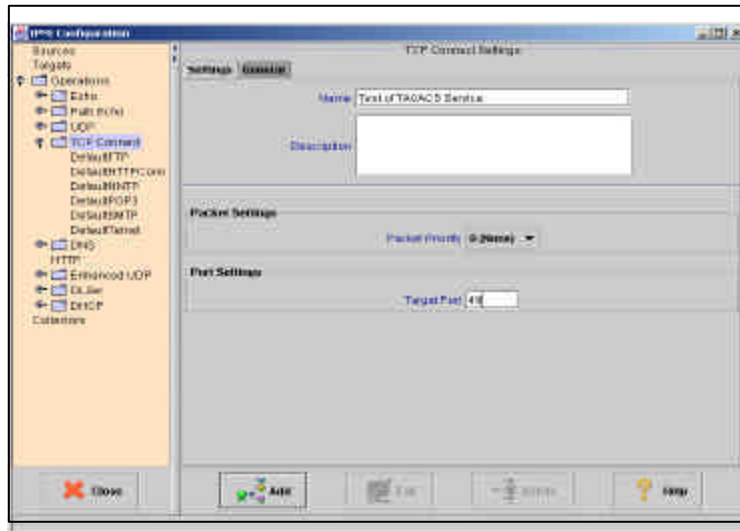
Action	Notes
Tested Link Between HA and FA With Pchar	Pchar Reports Bottleneck of 100mbits
Tested Link Between HA and TACACS+ Server With Pchar	Pchar Reports Bottleneck of 40mbit
Used IPM to Config a SAA Operation on the HA to Test Overall Application-layer Latency Between the HA and the TACACS+ Server	We Need to Determine If the Sum of Network-layer Latency Plus TACACS Application-layer Latency Is Our Overall Bottleneck

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

101

Configuring an Operation

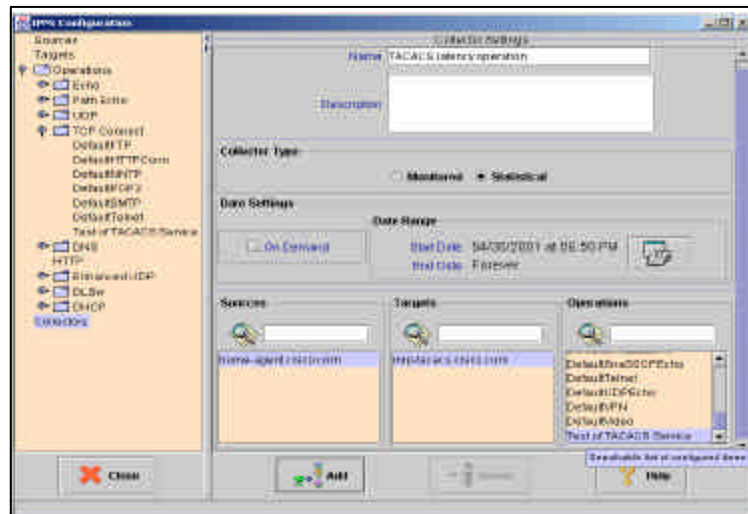
Cisco.com



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

102

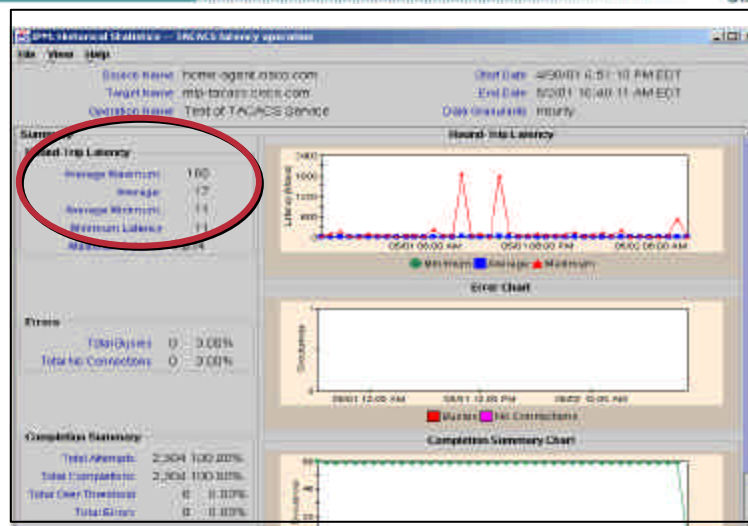
Configuring a Collector



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

103

Viewing the Results



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

104

Testing With the New Data

Cisco.com

- Ran lab tests with the new latency data from IPM/SAA
- Discovered that when many mobile nodes tried to register at once, latency spiked to unacceptable levels between the HA and the TACACS server
- This increase caused some mobile nodes to timeout when trying to register with the home agent

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

105

Problem Solved!

Cisco.com

Solution: Upgrading the path between the HA and the TACACS server along with upgrading the TACACS server's hardware allowed for more mobile node registrations to occur simultaneously without timeouts; upgrading the HA IOS to a version that cached registration requests also helped alleviate the problem

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

106

Summary and Tips

Cisco.com

- Don't panic!
- Understand your network
- Develop **network baselines**
- Gather the right information from your users
- Work methodically and document all your actions

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

107

Summary and Tips

Cisco.com

- Learn the tools
- Figure out which tools and which options work for each problem
- Use access-lists when enabling debug commands

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

108

Summary and Tips

Cisco.com

- Develop **network baselines**

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

109

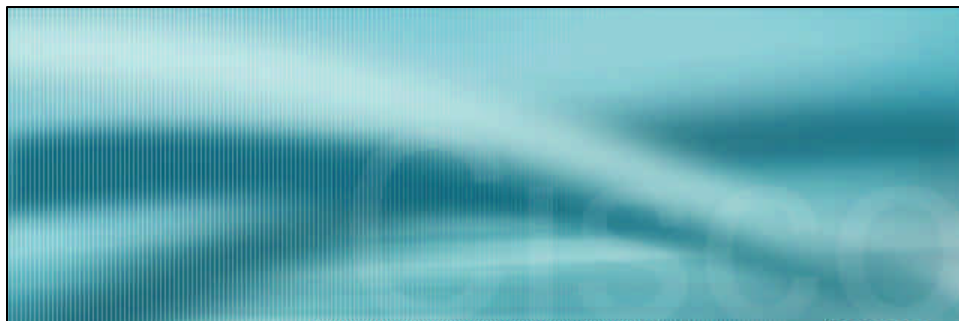
Network Troubleshooting Tools and Techniques

Session NCM-301

Cisco.com

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

110




Cisco.com

Please Complete Your Evaluation Form

Session NCM-301

NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

111



NCM-301
2945_05_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

112